VER. 2008 03 14 true

Korea Intellectual Property Office (KR) Registered Patent (B1)

KOREAN ENG.+KOR.

(51) Int.Cl. G06F 19/00

Published Date	2001-03-15		
Registration No	10-0284579		
Registration Date	2000-12-20		
Application No	10-1997-0072637	Unexamined Publication No	10-1999-0053067
Application Date	1997-12-23	Unexamined Publication Date	1999-07-15
Agent	KIM, Myong Sub LEE, Hwa Ik	Inventor	Cho Eun Kyung
Right Holder	Electronics and Telecommunications Research Institute		
Examiner	Eun-Cheol Lee		
Title of Invention	METHOD FOR ELECTRONICALLY PAYING SMALL SUM OF MONEY ON INTERNET		

Abstract

The present invention has the effect that as the thing about the small sum electronic payment base online service method making the small payment possible on internet, the user using the small sum electronic payment base online service is registered. E-cash is issued by using the hash function. And the small sum electronic payment base online service method for inexpensively performing the payment according to the use of service is provided. E-cash is transmitted for the electronic cash issue and use of service of the case of connecting with the internet mall and providing service even when being inexpensive to the hash function. The e-cash which it can use to the man reading advertisement or the man explaining the making up a question in the electronic commerce field of application in case of inquiring public opinion by advertiser or the making up a question is issued or it exchanges to the cash of the real life in case the constant price is. In that way the e-cash accelerates to see advertisement. The questionnaire number of respondent is increased. And the e-cash issuing can be induced to the electronic commerce use of service.

Description

Brief Explanation of the Drawing(s)

Fig. 1 is a process flow chart for the user registration, the process flow chart which E-cash Fig. 2 is issued, and Fig. 3 is the process flow chart for the use of service and payment according to the present invention.

〈The description of reference numerals of the main elements in drawings〉

10: buyer 20: payment center.

30: seller.

Details of the Invention

Purpose of the Invention

* The Technical Field to which the Invention belongs and the Prior Art in that Field

The present invention relates to the small sum electronic payment base online service method making the small payment possible on internet, particularly, to the small sum electronic payment base online service method it issues e-cash by using the hash function and for inexpensively performing the payment according to the use of service.

Recently, many concern devotes the electronic commerce field of application to the electronic commerce field of application among the online service field on internet. The internet mall in which the cost gives of the transaction money providing the news, the paper, the real estate information, including, the purchase of the information, the database retrieval, including, the charge charging, game, the sale of software of the low price like plug-in, including, service including newspaper, magazine etc. among this electronic commerce field of application one after another is expected to appear as the small sum. Therefore, the online service method by the suitable small sum method for electronic payment is required about this internet mall.

But presently, the online service method for the small sum electronic payment is not developed and the service of the internet mall is not used.

* The Technical Challenges of the Invention

There can be the purpose the e-cash issuing is induced to the electronic commerce use of service it exchanges, and in that way it accelerates to see advertisement, and the questionnaire number of respondent is increased as the cash of the real life in order to solve problem, the present invention registers the user using the small sum electronic payment base online service, and e-cash is issued by using the hash function, and the small sum electronic payment base online service method for inexpensively performing the payment according to the use of service is provided.

To accomplish the above objects, if the electronic cash issue the request (M1) by using the question number, including, the question number including the first process, of including the step the user registration (R1), and the step that the payment center tells the user registration it sends to the payment center the secret key which the buyer for to using the internet commerce produces is ciphered to the public key of the payment center and the advertisement, in which buyer answers the making up a question, quiz etc and response value using the same, by using the transaction identifier and publication cost etc., seller the response (M2) to buyer in the electronic cash issue request The step that the payment center tells the user registration cipher the sensitive information which the payment center produces according to buyer by using the secret key which buyer produces and it sends about the notification (R2). The second process, of being made of the step deciding on the payment center with the initialization (M3), the step that it transmits the Hash value toward the syzygy of the sensitive information Custom secret, the step that it transmits the Hash value about the syzygy of the money newScripType, the buyer transmitted e-cash is the step that tells about the result to the payment center after inspecting availability of e-cash, and the payment center termination stage where seller transmits the HTML document as the Response message toward the HTTP Request message of the payment server initialization phase (M3) to buyer after payment is successfully finished it transmits the transaction identifier the buyer receiving this to seller the service species which buyer

tries to purchase and the step that tells seller it uses the information about the service stored or not transmitted to browser, and the step that the seller receiving this tells the payment information of the target service buyer about the notification (S2). The step that it transmits the Hash value toward the syzygy of the sensitive information Custom secret the e-cash ScripType, held buyer and payment center share in the payment center and it performs the integrity and message authentication of e-cash and it publishes the publication of e-cash buyer with the initiation (M4). The step that it transmits the Hash value about the syzygy of the money newScripType is updated after examining the validity of e-cash and sensitive information Custom secret to buyer and the payment center receiving the e-cash issuing e-cash the publication (M5). The buyer receiving the notification of the target service is characterized that the step informing seller of the payment center initialization (S3), the e-cash of buyer, the step transmitting the Hash value for their syzygy and payment information in the payment center and the service charge the payment (S4), the step it diminishes the amount of money of e-cash after examining the validity of e-cash and that it measures and it publishes and it transmits the Hash value about the interview of the reissue money newScripType and sensitive information Custom secret to buyer and the payment center receiving this performs the payment processing (S5) of the service charge, the step that it plays the result watched the buyer transmitted e-cash to the payment center with the notification (S6) after watching the validity of e-cash, and the third process where it transmits the service are included in order to pay the service charge. The third process where it transmits the service buyer purchases seller as the Response message toward the HTTP Request message of the payment server initialization phase (S3) after payment is successfully finished.

- **Structure & Operation of the Invention**

The present invention relates to the small sum electronic payment base online service method, and as the thing about the online service method making the small payment possible in especially, internet, with the electronic cash issue protocol, the service request step, the service payment information notification step, the payment center initialization phase, the service charge payment step, the service charge payment processing level, the payment processing confirmation result notification step, consisting of the user registration protocol, the electronic cash issue challenge step, the electronic cash issue request-and-respond step, the payment center initialization phase, the electronic cash issue beginning stage, the electronic cash issue step, the e-cash confirmation, consisting of the user registration request stage and user registration notification step the result notification step and payment center termination stage the use of service and payment protocol are included.

The attached preferred embodiment is hereinafter particularly illustrated.

Fig. 1 provides the first step, and the second step which notifies buyer (10) of the user registration by using the user registration notification (R2) message this after the payment center (20) performs the user registration that the buyer (10) demands the user registration it transmits the user information with the payment center (20) it uses the user information registration request (R1) message the e-cash is issued service are generated it takes advantage of the time and the service which the user registration is especially once generated with the payment center (20) it takes advantage of the small sum electronic payment base online service it is the process flow chart for the user registration.

Firstly, in the first step, after the buyer (10) sets up the electronic wallet, the message (R1) demanding the user information entry of the payment center (20) is transmitted (101).

Here, the configuration of the R1 burn message is as follows.

The public key of the payment center (20) is same as those of the detail form of the R1 burn message is the following table (1) it is included in the electronic wallet distribution, and it is done by the private key in which it knows the secret key (KS) which the buyer (10) produces only the payment center (20) so that the user registration Huh cipher the R2 burn message of step.

Table 1

R1 burn message	
HeaderType	UM1: user registration request
ID	User electronic wallet identifier
Name	Registration user name
Address	Address
e-mail	Electronic mail address
etc	Miscellaneous information
KUcenter[KS]	The user registration Huh ciphers the R2 burn message of step The value ciphering the secret key (KS) to the public key (KUcenter) of the payment center

Next, the payment center (20) receiving the user information registration order message of above statement step (101) transmits the user registration notification message (R2) to the buyer (10). By using the secret key (KS) which the buyer (10) produces after the payment server registers user, the sensitive information (Custom Secret) which the payment center (20) especially produces with the buyer (10) is ciphered and it safely transmit (201)s. And the money value together transmits 0 persons e-cash with the R2 burn message. The detail form of the R2 burn message is same as those of the following table (2).

Table 2

R2 burn message	
HeaderType	UM2: user registration permission
ScripType	E-cash (ScripType)
KS[Custom_Secret]	Encoding the Custom Secret

As the process flow chart which E-cash Fig. 2 is issued, after the seller (30) in which the buyer (10) receives the first step, and the M1 message requesting the electronic cash issue to the seller (30) with the issue request (M1) message of e-cash after reading advertisement irradiates the response of the buyer (10) in other words to loosen the questionnaire response provided, and quiz in the internet mall etc., in case the validity are normal while performing the validity of e-cash by the fourth stage, transmitting the transaction ID and publication cost of the electronic cash issue etc. with the electronic cash issue permit information (M2) message to the buyer (10) and based transmits the Hash value about the syzygy of the second step, responding to the electronic cash issue request and the third step, and the e-cash ScripType, which initializes the payment center (20) as the seller (30) by transmitting the transaction ID with the payment server initialization (M3) message, and which the buyer (10) holds and the sensitive information Custom secret which the buyer (10) and payment center (20) share with the M4 message and performs the integrity and message authentication function of e-cash and discloses e-cash with publication and the payment center (20) receiving the M4 message with the Hash value inspection, money is made. The Hash value about the syzygy of the updated money newScripType and sensitive information Custom secret are transmitted with the e-

cash electrical transmission (M5) message to the buyer (10) and the integrity and message authentication function of e-cash are performed and the fifth step issuing e-cash, and the sixth step are included. The sixth step notifies of the e-cash confirmation and result it provides the authentication about the e-cash which the buyer (10) holds to the payment center (20) it transmits the e-cash which the buyer (10) possesses with the electronic cash issue termination (M6) message in the payment center (20) it performs the integrity of the e-cash which the payment center publishes etc. and the seventh step transmitting the electronic cash payment termination with the electronic cash payment termination (M7) to the buyer (10) and terminates the payment center (20).

Firstly, the detail form of the M1 burn message the electronic cash issue is in the first step through the M1 burn message the request (103) are same as those of the diagram below (3).

Table 3

M1 burn message	
HeaderType	GM1_ 1: electronic cash issue request
Item	The question number including advertisement, the making up a question, quiz etc.
Value	The response of the user according to service

In the second step, the message header transmits the GM2 1 or the GM2 2 phosphorus M2 burn message through the seller (30) in the browser of the buyer (10) after lower-part , and the payment center (20) irradiating the electronic cash issue require-message (M1) of the buyer (10) response through the M2 burn message in the electronic cash issue request. The message header the GM2 1 phosphorus M2 burn message means the electronic cash issue authorization. And the electronic cash issue information the data, in which it becomes the basis issuing e-cash as the information which the buyer (10) and payment center (20) share the message header the GM2 2 phosphorus M2 burn message transmits from the payment server in the form of the HTML document to publish e-cash to user (104). The detail form of the M2 burn message is same as those of the diagram below (4).

Table 4

M2 burn message	
HeaderType	GM2_ 1: electronic cash issue permit information
VendorId	The information of the internet mall ServerType
TranID	Transaction identifier
value	Publication cost
currency	Cash kinds
HeaderType	GM2_ 2: electronic cash issue not right information
HTML document	The electronic cash issue not right proprietary

In the third step, the payment center (20) is initialized through the M3 burn message. The M3 message is transmitted the buyer (10) transmitted the electronic cash issue request-and-respond with the seller (30) (105). The electronic cash issue initialization is performed. At this time, the detail form of the M3 burn message is same as those of the diagram below (5).

Table 5

M3 burn message

HeaderType	GM3_ 1: payment server initialization
TranID	Transaction identifier

In the fourth stage, the electronic cash issue is disclosed through the M4 burn message. It does not pass through the seller (30) with the M4 burn message which includes H [ScripType || Custom Secret] which is the Hash value about the sensitive information of e-cash and client in order to provide the integrity of e-cash besides the e-cash which holds and the buyer (10) directly starts the payment center (20) and electronic cash issue protocol (106). The detail form of the M4 burn message is same as those of the diagram below (6).

Table 6

M4 burn message	
HeaderType	GM4_ 1: electronic cash issue initiation
ScripType	It stores in the electronic wallet of user E-cash
H[ScripType || Custom_Secret]	The Hash value of the Custom Secret and ScripType
pCount	E-cash number of re-transmission
HeaderType	GM4_ 2: the electronic cash issue cancel

In the fifth step, E-cash is published through the M5 burn message. After the payment center (20) inspects the validity of the e-cash which the buyer (10) transmits, the amount of money of e-cash is increased as the publication cost included in the electronic cash issue information and reissue, and the e-cash measuring and issues the message header transmits e-cash through the GM5 1 phosphorus M5 burn message to the buyer (10) (107). And the message header is the case of issuing e-cash in case of the GM5 2, the GM5 3, and the GM5 4. The detail form of the M5 burn message is same as those of the diagram below (7).

Table 7

M5 burn message	
HeaderType	GM5_ 1: e-cash electrical transmission
newScripType	The e-cash in which the amount of money is updated
H(newScripType || Custom_Secret)	The Hash value of the Custom Secret and newScripType
pCount	E-cash number of re-transmission = 0
HeaderType	GM5_ 2: e-cash validity error
HeaderType	GM5_ 3: the electronic cash issue reject
HeaderType	GM5_ 4: payment server error
ScripType	The e-cash which user transmits
H(ScripType || Custom_Secret)	The Hash value of the Custom Secret and ScripType
pCount	pCount = pCount + 1

Here, while the cost giving in on characteristic small sum electronic payment of the small payment the fourth stage and fifth step is inexpensive, money has to be transmitted. Therefore, the public key cryptosystem or the shared key cryptosystem in which it very much requires the time and cost is not used. The integrity and message authentication service of e-cash are provided to the hash function.

In the sixth step, it notifies of the e-cash confirmation and result through the M6 burn message. The GM6 2 the validity is examined of the e-cash published in the payment center (20) is same as those of the detail form of the M6 burn message as the message header requesting the retransmiossion of e-cash by the buyer (10) detecting the e-cash validity error is the diagram below (8).

Table 8

M6 burn message	
HeaderType	GM6_ 1: electronic cash issue termination
HeaderType	GM6_ 2: e-cash request for retransmission
HeaderType	GM6_ 3: the electronic cash issue cancel
newScripType	The e-cash updated with the payment center
H(newScripType || Custom_Secret)	The Hash value of the Custom Secret and newScripType
pCount	pCount = pCount + 1

In the seventh step, it terminates through the M7 burn message with the payment center (20) and the electronic cash issue is terminated (109). In the internet mall with the response message about the payment center (20) initialization by the M3 burn message of the third step, it is the HTML document. The issue of money information or the service page can be selectively transmitted.

As Fig. 3 is the process flow chart for the use of service and payment, after the second step, transmitting the service payment electrical transmission (S2) message in which the first step, and the seller (30) in which the buyer (10) demands the service which the internet mall provides require the service charge payment about the use of service to the buyer (10) and notifies of the service payment information and the fourth stage, transmitting e-cash based on the service charge information which receives from the third step, and the S2 message transmitting the marker message which initializes the payment center (20) by distinguishing the transaction of the buyer (10) receiving the S2 message, with the seller (30) and initializes the payment center (20) with the order information with the payment processing confirmation (S4) message and pays the service charge and the payment center (20) receiving the S4 message reissue e-cash, the money updated based on the provided service charge with the S5 message is confirmed at the fifth step, and money and the S2 message which transmits the e-money balance electrical transmission (S5) message the e-cash which reissues with the Hash value with the sensitive information and handling the service charge payment held before the buyer (10) transmits the S5 message. The sixth step transmitting the grant whether or not of the e-cash which afresh is updated with the payment process termination (S6) message and notifies of the payment processing confirmation result and the seventh step transmitting the service which the buyer (10) selects are included.

In the first step, service is requested through the service purchase request (S1) message. By transmitting the information about the service for to purchasing and the service stored or not transmitted to browser with the S1 burn message each buyer (10) connected to the internet mall request purchase (110). The detail form of the S1 burn message is same as those of the diagram below (9).

Table 9

S1 burn message

HeaderType	PM1_ 1: service purchase request
Request-URL	The service which user purchases and user does
pMethod	The transmission mode selection of the service purchased (View or Save)

In the second step, the service payment information is notified of through the service payment electrical transmission (S2) message (111), here the header of message the PM2 1 phosphorus S2 burn message is the payment processing back-data between the payment information of the service which user tries to purchase the buyer (10) and the payment center (20). The header of message the PM2 2 phosphorus S2 burn message is the message which is transmitted to browser in case of dealing with the service which the buyer (10) purchases and it does. The detail form of the S2 burn message is same as those of the diagram below (10).

Table 10

S2 burn message	
HeaderType	PM2_ 1: service payment information
VendorId(ServerType)	The information of the internet mall
TranID	Transaction identifier
requestURL	The service for to purchasing
price	Cost
currency	Currency unit
deliveryMethod	The storing method of the service purchased (View or Save)
HeaderType	PM2_ 2: service suspension of sale
HTML document	The service sell serious consideration proprietary

In the third step, in order that the service charge is paid, the payment center (20) is initialized through the payment server initialization (S3) message. The detail form of the S3 burn message it transmits the S3 burn message with the seller (30) is same as those of the diagram below (11).

Table 11

S3 burn message	
HeaderType	PM3_ 1: payment server initialization
TranD	Transaction identifier

In the fourth stage, if the service charge is paid through the payment processing confirmation (S4) message, it connects the S2 message to the natural disposition to the payment center (20) and the buyer (10) transmits the charge payment message S4 for the service purchase (113). At this time, the detail form of the S4 burn message is same as those of the diagram below (12).

Table 12

S4 message	
HeaderType	PM4_ 1: the payment processing confirmation
ScripType	The e-cash stored in the electronic wallet of user
pOder	The payment information of the PM2 1 message

H(ScripType || pOder || Custom_Secret)	Scrip, and the Hash value of the pOder ,Custom Secret
pCount	E-cash number of re-transmission (= 0)
HeaderType	PM4_ 2: the payment processing cancel

The payment center (20) the validity is investigated of the e-cash in which the service charge is in the fifth step through the e-money balance electrical transmission (S5) message the payment processing (114), and which the buyer (10) makes payment are same as those of the message, in which it diminishes the amount of money of the e-cash in which the buyer (10) presents the payment information as the natural disposition and it reissues the e-cash corresponding to balance and the message header transmits the PM5 1 phosphorus S5 burn message, and the message header the PM5 2 , and the PM5 3 phosphorus S5 burn message is transmitted in case of processing payment. At this time, the detail form of the S5 burn message is the diagram below (13).

Table 13

S5 burn message	
HeaderType	PM5_ 1: e-money balance electrical transmission
newScripType	The e-cash in which the amount of money is updated
H[newScripType || Custom_Secret]	Of newScripType and Custom Secret Hash value
pCount	E-cash number of re-transmission (=0)
HeaderType	PM5_ 2: e-cash validity error
HeaderType	PM5_ 3: payment server error
ScripType	The e-cash which user makes payment
pOder	The payment information of the PM2 1 message
H[ScripType || pOder || Custom_Secret]	Of ScripType, and the pOder ,Custom Secret Hash value
pCount	pCount = pCount + 1

In the sixth step, the payment processing confirmation and result are told about the notification (115) through the payment process termination (S6) message. After the validity of the e-cash corresponding to balance is investigated after being transmitted through the payment processing of the payment center (20), in case error is detected, the message header PM6 2 phosphorus S6 burn message is transmitted and restart the payment processing. And the case of being normal terminates payment with the S6 message of the message header PM6 1. At this time, the detail form of the S6 burn message is same as those of the diagram below (13).

Table 14

S6 burn message	
HeaderType	PM6_ 1: payment process termination
HeaderType	PM6_ 2: e-cash request for retransmission
HeaderType	PM6_ 3: the payment processing failure
newScripType	The payment center publishes to balance E-cash

H[newScripType || Custom_Secret]	Of newScripType and Custom Secret Hash value
pCount	pCount = pCount + 1

In the seventh step, service is transmitted through the service transmission (S7) message in the general HTTP request message (116).

And the symbol used in the user registration protocol, and the electronic cash issue protocol, the use of service and payment protocol defines like next.

X shows the element of the small sum electronic payment base online service. And a || shows syzygy. KUx shows the public key of X. And KS shows the secure session key. The KUx [M] shows to cipher the message M to the public key KUx of X. The KS [M] shows the password box the message M in the secure session key KS. And H [M] shows the Hash value applying the hash function H the message M. The structure of the e-cash (ScripType) and the message header (HeaderType) which is used in order to describe message defines like the diagram below (14).

Table 15

Message header structure: headerType		
cmdType	The type of header, a lot, the UM (user registration) message To the GM (electronic cash issue) message, and the PM (the payment processing) message It is classified	
protocolVersion	The Version information of the small sum electronics payment protocol	
serverDate	Protocol performance time	
errorMessage	The general error message	
E-cash structure: scripType		
E-cash (ScripType)	HashAlgorithm	Hash algorithm identifier
scrip	The data construct of ScripBodyType	
certificate	E-cash certificate	
ScripBodyType	currency	Currency unit
value	The amount of money of e-cash	
VendorId	The data construct of ServerType	
ScripId	The issue of money information-identification with IdType	

CustomId	The Custom Secret information of issue with IdType	
Ad	The service identifier including advertisement, the making up a question etc. Field	
expirationDate	E-cash term of validity	
ServerType	DnsName	The domain of the payment server
IpAddr	IP address	
ServerName	Internet mall reciprocity	
port	Payment server port number	
IdType	secretId	The identifier of the sensitive information
serialNumber	Serial number	

As described above, the small sum electronic payment base online service method has the effect that E-cash is safely transmitted for the electronic cash issue and use of service of the case of connecting with the internet mall and providing service even when being inexpensive to the hash function. The e-cash which it can use to the man reading advertisement or the man explaining the making up a question in the electronic commerce field of application in case of inquiring public opinion by advertiser or the making up a question is issued or it exchanges to the cash of the real life in case the constant price is. In that way the e-cash accelerates to see advertisement. The questionnaire number of respondent is increased. And the e-cash issuing can be induced to the electronic commerce use of service.

- **Effects of the Invention**

The present invention has the effect that the user using the small sum electronic payment base online service is registered. E-cash is issued by using the hash function. And the small sum electronic payment base online service method for inexpensively performing the payment according to the use of service is provided. E-cash is transmitted for the electronic cash issue and use of service of the case of connecting with the internet mall providing the news, the paper, the real estate information, including, the purchase of the information, the database retrieval, including, the charge charging, game, the sale of software of the low price like plug-in, including, service including newspaper, magazine etc. among the electronic commerce field of application decreasing the e-cash of the small sum and uses this and providing service even when being inexpensive to the hash function. The e-cash which it can use to the man reading advertisement or the man explaining the making up a question in the electronic commerce field of application in case of inquiring public opinion by advertiser or the making up a question is issued or it exchanges to the cash of the real life in case the constant price is. In that way the e-cash accelerates to see advertisement. The questionnaire number of respondent is increased. And the e-cash issuing can be induced to the electronic commerce use of service.

Scope of Claims

Claim[1] :

If the electronic cash issue is the request (M1) by using the question number, including, the question number including the first process: advertisement, in which buyer answers the making up a question, quiz etc. of including the step the user registration (R1), and the step that the payment center tells the user registration it sends to the payment center the secret key which the buyer for to using the internet commerce produces is ciphered to the public key of the payment center and response value using the same, by using the transaction identifier and publication cost etc., seller the response (M2) to buyer in the electronic cash issue request. The step that the payment center tells the user registration cipher the sensitive information which the payment center produces according to buyer by using the secret key which buyer produces and it sends about the notification (R2). The second process:, of being made of the step deciding on the payment center with the initialization (M3), the step that it transmits the Hash value toward the syzygy of the sensitive information Custom secret, the step that it transmits the Hash value about the syzygy of the money newScripType, the buyer transmitted e-cash is the step that tells about the result to the payment center after inspecting availability of e-cash, and the payment center termination stage where seller transmits the HTML document as the Response message toward the HTTP Request message of the payment server initialization phase (M3) to buyer after payment is successfully finished it transmits the transaction identifier the buyer receiving this to seller the service species which buyer tries to purchase and the step that tells seller it uses the information about the service stored or not transmitted to browser, and the step that the seller receiving this tells the payment information of the target service buyer about the notification (S2). The step that it transmits the Hash value toward the syzygy of the sensitive information Custom secret the e-cash ScripType, held buyer and payment center share in the payment center and it performs the integrity and message authentication of e-cash and it publishes the publication of e-cash buyer with the initiation (M4). The step that it transmits the Hash value about the syzygy of the money newScripType is updated after examining the validity of e-cash and sensitive information Custom secret to buyer and the payment center receiving the e-cash issuing e-cash the publication (M5). The small sum electronic payment base online service method wherein the buyer receiving the notification of the target service includes the step, that informs seller of the payment center initialization (S3) it pays the service charge the e-cash of buyer, the step, that the service charge the payment (S4) the step, transmits the Hash value for their syzygy and payment information in the payment center the step, that performs the service charge payment processing (S5) the payment center receiving this transmits the Hash value about the interview of the reissue money newScripType and sensitive information Custom secret to buyer the validity reissues it diminishes the amount of money of e-cash it examines the validity of e-cash the step that tells about the result watched to the payment center it watches the validity of e-cash the buyer transmitted e-cash, and the third process where it transmits the service which buyer purchases seller as the Response message toward the HTTP Request message of the payment server initialization phase (S3) after payment is finished.

Representative Drawing(s)

Fig. 2

Legal Status

Date	Type of Document	Status
19971223	Application of Patent	Received
19971223	Request for Examination	Received
20000128	Notice of Submission of Opinion	Delivery Completed

20000328	Submission of opinion	Received
20000328	Amendment including Specification etc.	Amendment Approved
20001128	Written Decision on Registration	Delivery Completed

특1999-0053067

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 19/00

(11) 공개번호 특1999-0053067
(43) 공개일자 1999년07월15일

(21) 출원번호 10-1997-0072637
(22) 출원일자 1997년12월23일

(71) 출원인 한국전자통신연구원 정선종
대전광역시 유성구 가정동 161번지
(72) 발명자 조은경
대전광역시 유성구 어은동 99번지 한빛아파트 112동 503호
(74) 대리인 김명섭, 이화익

심사청구 : 있음

(54) 소액 전자 지불 기반 온라인 서비스 방법

요약

본 발명은 인터넷 상에서 소액 지불을 가능하게 하는 소액 전자 지불 기반 온라인 서비스 방법에 관한 것으로서, 소액 전자 지불 기반 온라인 서비스를 사용하는 사용자를 등록하고, 해쉬 함수를 이용하여 전자 화폐를 발행하며, 서비스 이용에 따른 대금 지불을 저렴하게 수행하는 소액 전자 지불 기반 온라인 서비스 방법을 제공하여, 인터넷 상점과 연계하여 서비스를 제공하는 경우의 전자 화폐 발행 및 서비스 이용을 위해 해쉬 함수만으로 저렴하면서도 안전하게 전자 화폐를 전송하여, 광고주나 설문에 의한 여론 조사를 하는 경우 광고를 읽는 사람이나 설문에 대답하는 사람에게 전자 상거래 응용 분야에서 사용할 수 있는 전자 화폐를 발행하거나 일정 금액이 되는 경우 실세계의 현금으로 환전하여 줌으로써, 광고를 보는 것을 촉진시키고, 설문지 응답자 수를 증가시키며, 발행된 전자 화폐를 전자 상거래 서비스 이용으로 유도할 수 있는 효과가 있다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 사용자 등록을 위한 처리 흐름도,

도 2는 본 발명에 따른 전자 화폐를 발행 받기 위한 처리 흐름도,

도 3은 서비스 이용 및 지불을 위한 처리 흐름도.

〈도면의 주요 부분에 대한 부호의 설명〉

10 : 구매자 20 : 지불 센터

30 : 판매자

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 인터넷 상에서 소액 지불을 가능하게 하는 소액 전자 지불 기반 온라인 서비스 방법에 관한 것으로서, 특히, 해쉬 함수를 이용하여 전자 화폐를 발행하고 서비스 이용에 따른 대금 지불을 저렴하게 수행하는 소액 전자 지불 기반 온라인 서비스 방법에 관한 것이다.

최근 인터넷 상의 온라인 서비스 분야 중에서 전자 상거래 응용 분야에 많은 관심이 기울여지고 있다. 이러한 전자 상거래 응용 분야 중 신문, 잡지 등의 기사, 논문, 부동산 정보 등과 같은 정보의 구매, 데이터베이스 검색 등과 같은 이용료 과금, 게임, 플러그인과 같은 저가격의 소프트웨어 판매 등과 같은 서비스를 제공하는 거래 금액이 소액으로 그 비용이 적게 드는 인터넷 상점이 속속 등장할 것으로 예상되어진다. 따라서, 이러한 인터넷 상점에 대해 적합한 소액 전자 지불 방법에 의한 온라인 서비스 방법이 요구되고 있다.

9-1

그러나, 현재 소액 전자 지불을 위한 온라인 서비스 방법이 개발되지 않아 인터넷 상점의 서비스가 활용되지 못하고 있다.

발명이 이루고자 하는 기술적 과제

상기 문제점을 해결하기 위해 본 발명은, 소액 전자 지불 기반 온라인 서비스를 사용하는 사용자를 등록하고, 해쉬 함수를 이용하여 전자 화폐를 발행하며, 서비스 이용에 따른 대금 지불을 저렴하게 수행하는 소액 전자 지불 기반 온라인 서비스 방법을 제공하여, 광고주나 설문에 의한 여론 조사를 하는 경우 광고를 읽는 사람이나 설문에 대답하는 사람에게 전자 상거래 응용 분야에서 사용할 수 있는 전자 화폐를 발행하거나 일정 금액이 되는 경우 실세계의 현금으로 환전하여 줌으로써, 광고를 보는 것을 촉진시키고, 설문지 응답자 수를 증가시키며, 발행된 전자 화폐를 전자 상거래 서비스 이용으로 유도하는데 그 목적이 있다.

발명의 구성 및 작용

본 발명은 소액 전자 지불 기반 온라인 서비스 방법에 관한 것으로, 특히, 인터넷에서 소액 지불 을 가능하게 하는 온라인 서비스 방법에 관한 것으로서, 사용자 등록 요구 단계 및 사용자 등록 통지 단계로 이루어진 사용자 등록 프로토콜과, 전자 화폐 발행 요청 단계, 전자 화폐 발행 요청 응답 단계, 지불 센터 초기화 단계, 전자 화폐 발행 개시 단계, 전자 화폐 발행 단계, 전자 화폐 확인 및 결과 통지 단계 및 지불 센터 종료 단계로 이루어진 전자 화폐 발행 프로토콜과, 서비스 요청 단계, 서비스 지불 정보 통지 단계, 지불 센터 초기화 단계, 서비스 이용료 지불 단계, 서비스 이용료 지불 처리 단계, 지불 처리 확인 결과 통지 단계 및 서비스 이용 및 지불 프로토콜을 포함한다.

이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명한다.

도 1 은 본 발명에 따른 사용자 등록을 위한 처리 흐름도로서, 사용자 등록은 소액 전자 지불 기반 온라인 서비스를 이용하기 전에 지불 센터(20) 별로 한번 발생하며, 전자 화폐를 발행 받을 때와 서비스를 이용할 때 각각 발생하게 되고, 구매자(10)가 사용자 정보를 R1 메시지를 이용하여 지불 센터(20)로 전송하여 사용자 등록을 요구하는 제 1 단계와, 지불 센터(20)가 사용자 등록을 수행한 후 이를 R2 메시지를 이용하여 구매자(10)에게 사용자 등록을 통지하는 제 2 단계를 포함한다.

먼저, 상기 제 1 단계에서는 구매자(10)가 전자 지갑을 설치한 후, 지불 센터(20)로 사용자 정보 등록을 요구하는 메시지(R1)를 송출한다(101).

여기서, 상기 R1번 메시지의 구성은 다음과 같다.

지불 센터(20)의 공개키는 전자 지갑 배포시 포함되고, 사용자 등록 허가 단계의 R2번 메시지를 암호화하기 위해 구매자(10)가 생성한 비밀키(KS)를 지불 센터(20)만이 아는 개인키로 하여, 지불 센터(20)만이 복호화할 수 있도록 지불 센터(20)의 공개키(KUcenter)로 암호화한 값을 R1번 메시지로 전송하며, R1번 메시지의 세부 형식은 다음의 표(1)과 같다.

[표 1]

R1번 메시지	
HeaderType	UM1 : 사용자 등록 요청
ID	사용자 전자 지갑 식별자
Name	등록 사용자 이름
Address	주소
e-mail	전자 우편 주소
etc	기타 정보
KUcenter[KS]	사용자 등록 허가 단계의 R2번 메시지를 암호화하기 위한 비밀키(KS)를 지불 센터의 공개키(KUcenter)로 암호화한 값

다음으로, 상기 단계(101)의 사용자 정보 등록 요구 메시지를 수신한 지불 센터(20)가 상기 구매자(10)에게 사용자 등록 통지 메시지(R2)를 전송하는데(201), 지불서버는 사용자 등록을 한 후 구매자(10)가 생성한 비밀키(KS)를 사용해 지불 센터(20)가 구매자(10) 별로 생성한 비밀 정보(Custom_Secret)를 암호화해서 안전하게 전송한다. 그리고, 화폐가치는 0인 전자 화폐를 함께 R2번 메시지로 전송한다. R2번 메시지의 세부 형식은 다음의 표(2)와 같다.

[표 2]

R2 번 메시지	
HeaderType	UM2 : 사용자 등록 허가
ScripType	전자화폐(ScripType)
KS[Custom_Secret]	Custom_Secret를 암호화

도 2 는 본 발명에 따른 전자화폐를 발행 받기 위한 처리 흐름도로서, 인터넷 상점 등에서 제공하는 설문

9-2

지 응답, 퀴즈 풀기 또는 광고를 읽은 후 구매자(10)가 M1 메시지에 의해 판매자(30)에게 전자화폐 발행을 요청하는 제 1 단계와, 상기 M1 메시지를 수신한 판매자(30)가 상기 구매자(10)의 응답을 조사한 후, 전자화폐 발행의 근거가 되는 트랜잭션 ID와 발행 금액 등을 M2 메시지에 의해 상기 구매자(10)에게 전송하여 전자화폐 발행 요청에 응답하는 제 2 단계와, 지불 센터(20)로 트랜잭션 ID를 M3 메시지로 전송하므로써 지불 센터(20)를 초기화하는 제 3 단계와, 상기 구매자(10)가 보유하고 있는 전자화폐 ScripType와, 구매자(10)와 지불 센터(20)가 공유하는 비밀 정보 Custom_secret의 연접에 대한 해쉬 값을 M4 메시지로 전송하여 전자화폐의 무결성 및 메시지 인증 기능을 수행하여 전자화폐를 발행 개시하는 제 4 단계와, 상기 M4 메시지를 수신한 상기 지불 센터(20)에 의한 전자화폐의 유효성을 해쉬 값 검사에 의해 수행하며 정상적인 경우 화폐를 갱신하고, 갱신된 화폐 newScripType와 비밀 정보 Custom_secret의 연접에 대한 해쉬 값을 M5 메시지로 상기 구매자(10)에게 전송하여 전자화폐의 무결성 및 메시지 인증 기능을 수행하여 전자화폐를 발행하는 제 5 단계와, 상기 지불 센터가 발행한 전자화폐의 무결성등을 수행한 후, 구매자(10)가 보유하는 전자화폐를 지불 센터(20)에 M6 메시지로 전송하여 상기 지불 센터(20)로 하여금 상기 구매자(10)가 보유하는 전자화폐에 대한 인증을 제공하여 전자화폐 확인 및 결과를 통지하는 제 6 단계 및 전자화폐 지불 종료를 M7에 의해 상기 구매자(10)에게 전송하여 지불 센터(20)를 종료하는 제 7 단계를 포함한다.

먼저, 상기 제 1 단계에서는 M1번 메시지를 통하여 전자화폐 발행을 요청(103)하는데, M1번 메시지의 세부 형식은 하기 표(3)과 같다.

[표 3]

M1 번 메시지	
HeaderType	GM1_1 : 전자화폐 발행 요청
Item	광고, 설문, 퀴즈 등의 문제 번호
Value	서비스에 따른 사용자의 응답

상기 제 2 단계에서는 M2번 메시지를 통하여 전자화폐 발행 요청에 응답을 한다. 지불 센터(20)는 구매자(10)의 전자화폐 발행 요청 메시지(M1)를 조사한 후 메시지 헤더가 GM2_1 또는 GM2_2 인 M2번 메시지를 판매자(30)를 통해 구매자(10)의 브라우저에 전송한다. 메시지 헤더가 GM2_1인 M2번 메시지는 전자화폐 발행 허가를 의미하며, 전자화폐 발행 정보는 구매자(10)와 지불 센터(20)가 서로 공유하는 정보로써 전자화폐를 발행하는 근거가 되는 데이터이다. 메시지 헤더가 GM2_2인 M2번 메시지는 지불서버에서 사용자에게 전자화폐를 발행해 줄 수 없음을 HTML 문서의 형태로 전송한다(104). M2번 메시지의 세부 형식은 하기 표(4)와 같다.

[표 4]

M2번 메시지	
HeaderType	GM2_1 : 전자화폐 발행 허가 정보
VendorId	인터넷 상점의 정보로 ServerType임
TranID	트랜잭션 식별자
value	발행 금액
currency	화폐 종류
HeaderType	GM2_2 : 전자화폐 발행 불가 정보
HTML 문서	전자화폐 발행 불가 사유

상기 제 3 단계에서는 M3번 메시지를 통하여 지불 센터(20)를 초기화한다. 전자화폐 발행 요청 응답을 전송 받은 구매자(10)는 M3 메시지를 지불 센터(20)로 전송하여(105), 전자화폐 발행 초기화를 수행 할 수 있도록한다. M3번 메시지의 세부 형식은 하기 표(5)와 같다.

[표 5]

M3번 메시지	
HeaderType	GM3_1 : 지불서버 초기화
TranID	트랜잭션 식별자

상기 제 4 단계에서는 M4번 메시지를 통하여 전자화폐 발행을 개시한다. 구매자(10)는 보유하고 있는 전자화폐 외에도 전자화폐의 무결성을 제공하기 위해 전자화폐와 고객의 비밀 정보에 대한 해쉬값인 H[ScripType || Custom_Secret]를 포함하는 M4번 메시지에 의해 판매자(30)를 경유하지 않고 직접 지불 센터(20)와 전자화폐 발행 프로토콜을 시작한다(106). M4번 메시지의 세부 형식은 하기 표(6)과 같다.

9-3

[표 6]

M4번 메시지	
HeaderType	GM4_1 : 전자화폐 발행 개시
ScripType	사용자의 전자지갑에 저장하고 있는 전자화폐
H[ScripType || Custom_Secret]	ScripType과 Custom_Secret의 해쉬값
pCount	전자화폐 재전송 횟수
HeaderType	GM4_2 : 전자화폐 발행 취소

상기 제 5 단계에서는 M5번 메시지를 통하여 전자화폐를 발행한다. 지불 센터(20)는 구매자(10)가 전송한 전자화폐의 유효성을 검사한 후, 전자화폐 발행 정보에 포함된 발행 금액만큼 전자화폐의 금액을 증가시켜 전자화폐를 재발행 하고, 재 발행된 전자화폐는 메시지헤더가 GM5_1인 M5번 메시지를 통해 구매자(10)에게 전송한다(107). 메시지 헤더가 GM5_2, GM5_3, GM5_4 각각의 경우는 전자화폐를 발행해 줄 수 없는 경우이다. M5번 메시지의 세부 형식은 하기 표(7)과 같다.

[표 7]

M5번 메시지	
HeaderType	GM5_1 : 전자화폐 전송
newScripType	금액이 갱신된 전자화폐
H(newScripType || Custom_Secret)	newScripType과 Custom_Secret의 해쉬값
pCount	전자화폐 재전송 횟수 = 0
HeaderType	GM5_2 : 전자화폐 유효성 오류
HeaderType	GM5_3 : 전자화폐 발행 거절
HeaderType	GM5_4 : 지불서버 오류
ScripType	사용자가 전송한 전자화폐
H(ScripType || Custom_Secret)	ScripType과 Custom_Secret의 해쉬값
pCount	pCount = pCount + 1

여기서, 상기 제 4 단계 및 제 5 단계는 소액 지불의 특성상 소액 전자 지불에 드는 비용이 저렴하면서 안전하게 화폐가 전송되어야 하므로, 시간 및 비용이 많이 드는 공개키 암호 시스템 또는 공유키 암호 시스템을 사용하지 않고, 해쉬 함수만으로 전자화폐의 무결성 및 메시지 인증 서비스를 제공하고 있다.

상기 제 6 단계에서는 M6번 메시지를 통하여 전자화폐 확인 및 결과 통지를 한다. 지불 센터(20)에서 발행한 전자화폐의 유효성을 검사한 후, 이 결과에 따라 지불 센터(20)에 M6 메시지를 전송한다(108). 정상적인 경우 메시지의 헤더가 GM6_1인 M6번 메시지를 지불 센터(20)에 전송하며, GM6_2는 전자화폐 유효성 오류를 검출한 구매자(10)에 의한 전자화폐의 재전송을 요구하는 메시지 헤더이다. M6번 메시지의 세부 형식은 하기 표(8)과 같다.

[표 8]

M6번 메시지	
HeaderType	GM6_1 : 전자화폐 발행 종료
HeaderType	GM6_2 : 전자화폐 재전송 요구
HeaderType	GM6_3 : 전자화폐 발행 취소
newScripType	지불 센터에 의해 갱신된 전자화폐
H(newScripType || Custom_Secret)	newScripType과 Custom_Secret의 해쉬값
pCount	pCount = pCount + 1

상기 제 7 단계에서는 M7번 메시지를 통하여 지불 센터(20) 종료하여 전자화폐 발행을 종료한다(109). 상기 제 3 단계의 M3번 메시지에 의한 지불 센터(20) 초기화에 대한 응답 메시지로써 인터넷 상점에서 HTML 문서이다. 화폐 발행 정보 또는 서비스 페이지를 선택적으로 전송할 수 있다.

도 3 은 서비스 이용 및 지불을 위한 처리 흐름도로서, 구매자(10)가 인터넷 상점이 제공하는 서비스를 요청하는 제 1 단계와, 판매자(30)가 서비스 이용에 대한 서비스 이용료 지불을 요구하는 S2 메시지를 상기 구매자(10)에게 전송하여 서비스 지불 정보를 통지하는 제 2 단계와, S2 메시지를 수신한 구매자(10)의 트랜잭션을 식별하므로써 지불 센터(20)를 초기화하는 S3 메시지를 지불 센터(20)로 전송하여 지불 센터(20)를 초기화하는 제 3 단계와, 상기 S2 메시지로부터 수신한 서비스 이용료 정보에 근거하여 주문 정보와

9-4

함께 전자화폐를 S4 메시지로 전송하여 서비스 이용료를 지불하는 제 4 단계와, 상기 S4 메시지를 수신한 지불 센터(20)가 전자화폐를 재발행한 후, 재발행한 전자화폐를 비밀 정보와의 해쉬값으로 S5 메시지를 전송하여 서비스 이용료를 지불 처리하는 제 5 단계와, 상기 구매자(10)가 S5 메시지를 전송하기전에 보유하고 있던 화폐와 상기 S2 메시지에서 제공된 서비스 이용료에 근거하여 상기 S5 메시지에 의해 갱신된 화폐를 확인하고, 새로이 갱신된 전자화폐의 수락 여부를 S6 메시지에 의해 전송하여 지불 처리 확인 결과를 통지하는 제 6 단계 및 상기 구매자(10)가 선택한 서비스를 전송하는 제 7 단계를 포함한다.

상기 제 1 단계에서는 S1번 메시지를 통하여 서비스를 요청한다. 인터넷 상점에 연결한 각 구매자(10)들은 구매하고자 하는 서비스와 브라우저로 전송되는 서비스 저장 여부에 관한 정보를 S1번 메시지로 전송하므로써 구매 요청을 한다(110). S1번 메시지의 세부 형식은 하기 표(9)와 같다.

[표 9]

S1번 메시지	
HeaderType	PM1_1 : 서비스 구매 요청
Request-URL	사용자가 구매하고 하는 서비스
pMethod	구매한 서비스의 전송형태 선택 (View or Save)

상기 제 2 단계에서는 S2번 메시지를 통하여 서비스 지불 정보를 통지한다(111). 여기서, 메시지의 헤더가 PM2_1인 S2번 메시지는 사용자가 구매하고자 하는 서비스의 지불 정보이며, 구매자(10)와 지불 센터(20) 사이의 지불 처리 근거 데이터이다. 메시지의 헤더가 PM2_2인 S2번 메시지는 구매자(10)가 구매하고 하는 서비스를 판매할 수 없을 경우 브라우저로 전송되는 메시지이다. S2번 메시지의 세부 형식은 하기 표(10)과 같다.

[표 10]

S2번 메시지	
HeaderType	PM2_1 : 서비스 지불 정보
VendorId(ServerType)	인터넷 상점의 정보
TranID	트랜잭션 식별자
requestURL	구매하고자 하는 서비스
price	가격
currency	화폐 단위
deliveryMethod	구매한 서비스의 저장 방법 (View or Save)
HeaderType	PM2_2 : 서비스 판매 중지
HTML 문서	서비스 판매 중지 사유

상기 제 3 단계에서는 서비스 이용료를 지불하기 위해, S3번 메시지를 통하여 지불 센터(20)를 초기화한다. S2번 메시지에 의해 서비스 지불 정보를 전송 받은 구매자(10)는 S3번 메시지를 지불 센터(20)로 전송하여 지불 처리를 위한 지불 센터(20) 초기화를 한다(112). S3번 메시지의 세부 형식은 하기 표(11)과 같다.

[표 11]

S3번 메시지	
HeaderType	PM3_1 : 지불서버 초기화
TranD	트랜잭션 식별자

상기 제 4 단계에서는 S4번 메시지를 통하여 서비스 이용료를 지불한다 구매자(10)는 S2 메시지를 바탕으로 지불 센터(20)에 연결하여 서비스 구매를 위한 이용료 지불 메시지 S4를 송신한다(113). S4번 메시지의 세부 형식은 하기 표(12)와 같다.

[표 12]

S4 메시지	
HeaderType	PM4_1 : 지불처리 확인
ScripType	사용자의 전자지갑에 저장하고 있는 전자화폐
pOder	PM2_1 메시지의 지불 정보

9-5

H(ScripType || pOder || Custom_Secret)	Scrip, pOder ,Custom_Secret의 해쉬값
pCount	전자화폐 재전송 횟수(= 0)
HeaderType	PM4_2 : 지불 처리 취소

상기 제 5 단계에서는 S5번 메시지를 통하여 서비스 이용료를 지불 처리(114)하는데, 구매자(10)가 지불한 전자화폐의 유효성을 조사한 후, 지불 센터(20)는 지불 정보를 바탕으로 구매자(10)가 제시한 전자화폐의 금액을 감소시켜 잔액에 해당하는 전자화폐를 재발행하여 메시지 헤더가 PM5_1인 S5번 메시지를 전송한다. 메시지 헤더가 PM5_2, PM5_3 인 S5번 메시지는 지불 처리를 할 수 없을 경우 전송되는 메시지이다. S5번 메시지의 세부 형식은 하기 표(13)과 같다.

[표 13]

S5번 메시지	
HeaderType	PM5_1 : 전자화폐 잔액 전송
newScripType	금액이 갱신된 전자화폐
H[newScripType || Custom_Secret]	newScripType과 Custom_Secret의 해쉬값
pCount	전자화폐 재전송 횟수(=0)
HeaderType	PM5_2 : 전자화폐 유효성 오류
HeaderType	PM5_3 : 지불서버 오류
ScripType	사용자가 지불한 전자화폐
pOder	PM2_1 메시지의 지불정보
H[ScripType || pOder || Custom_Secret]	ScripType, pOder ,Custom_Secret의 해쉬값
pCount	pCount = pCount + 1

상기 제 6 단계에서는 S6번 메시지를 통하여 지불 처리 확인 및 결과를 통지(115) 하는데, 지불 센터(20)의 지불 처리를 통해 전송 받은 후 잔액에 해당하는 전자화폐의 유효성을 조사한 후, 오류가 검출될 경우 메시지 헤더 PM6_2 인 S6번 메시지를 전송하여 지불 처리를 재시도 한다. 정상적인 경우는 메시지 헤더 PM6_1의 S6범 메시지에 의해 지불을 종료한다. S6번 메시지의 세부 형식은 하기 표(13)과 같다.

[표 14]

S6번 메시지	
HeaderType	PM6_1 : 지불처리 종료
HeaderType	PM6_2 : 전자화폐 재전송 요구
HeaderType	PM6_3 : 지불처리 실패
newScripType	지불 센터가 잔액으로 발행한 전자화폐
H[newScripType || Custom_Secret]	newScripType과 Custom_Secret의 해쉬값
pCount	pCount = pCount + 1

상기 제 7 단계에서는 S7번 메시지를 통하여 일반적인 HTTP request 메시지에 서비스를 전송한다(116).

그리고, 상기 사용자 등록 프로토콜, 전자화폐 발행 프로토콜 및 서비스 이용 및 지불 프로토콜에서 사용되는 기호는 다음과 같이 정의한다.

X는 소액 전자 지불 기반 온라인 서비스의 구성 요소를 나타내며, ||는 연접을 나타낸다. KUx는 X의 공개키를 나타내며, KS는 비밀세션키를 나타낸다. KUx[M]은 메시지 M을 X의 공개키 KUx로 암호화함을 나타내고, KS[M]은 메시지 M을 비밀 세션키 KS로 암호함을 나타낸다. H[M]은 메시지 M을 해쉬함수 H를 적용한 해쉬 값을 나타낸다. 그리고, 메시지를 기술하기 위해 사용되는 메시지 헤더(HeaderType)와 전자화폐(ScripType)의 구조는 하기 표(14)와 같이 정의한다.

9-6

[표 15]

메시지 헤더 구조 : HeaderType			
cmdType	헤더의 타입으로써 크게 UM(사용자 등록) 메시지, GM(전자화폐 발행) 메시지, PM(지불처리) 메시지로 구분된다.		
protocolVersion	소액 전자 지불 프로토콜의 버전 정보		
serverDate	프로토콜 수행 시각		
errorMessage	일반적인 오류 메시지		
	전자화폐 구조 : ScripType		
전자화폐 (ScripType)	HashAlgorithm	해쉬알고리즘 식별자	
	scrip	ScripBodyType의 데이터 구조	
	certificate	전자화폐 인증서	
ScripBodyType	currency	화폐 단위	
	value	전자화폐의 금액	
	VendorId	ServerType의 데이터 구조	
	ScripId	IdType으로써 화폐 발행 정보 식별자	
	CustomId	IdType으로써 Custom_Secret 발행정보	
	Ad	광고,설문 등과 같은 서비스 식별자 필드	
	expirationDate	전자화폐 유효기간	
ServerType	DnsName	지불서버의 도메인	
	IpAddr	IP 주소	
	ServerName	인터넷 상점 상호	
	port	지불서버 포트 번호	
IdType	secretId	비밀정보의 식별자	
	serialNumber	일련번호	

상기와 같이 본 발명에 따른 소액 전자 지불 기반 온라인 서비스 방법은 인터넷 상점과 연계하여 서비스를 제공하는 경우의 전자화폐 발행 및 서비스 이용을 위해 해쉬 함수만으로 저렴하면서도 안전하게 전자화폐를 전송하여, 광고주나 설문에 의한 여론 조사를 하는 경우 광고를 읽는 사람이나 설문에 대답하는 사람에게 전자 상거래 응용 분야에서 사용할 수 있는 전자화폐를 발행하거나 일정 금액이 되는 경우 실세계의 현금으로 환전하여 줌으로써, 광고를 보는 것을 촉진시키고, 설문지 응답자 수를 증가시키며, 발행된 전자화폐를 전자 상거래 서비스 이용으로 유도할 수 있는 효과가 있다.

발명의 효과

본 발명은 소액 전자 지불 기반 온라인 서비스를 사용하는 사용자를 등록하고, 해쉬 함수를 이용하여 전자화폐를 발행하며, 서비스 이용에 따른 대금 지불을 저렴하게 수행하는 소액 전자 지불 기반 온라인 서비스 방법을 제공하여, 소액의 전자 화폐를 주고 이를 이용하는 전자 상거래 응용 분야 중 신문, 잡지 등의 기사, 논문, 부동산 정보 등과 같은 정보의 구매, 데이터베이스 검색 등과 같은 이용료 과금, 게임, 플러그인과 같은 저가격의 소프트웨어 판매 등과 같은 서비스를 제공하는 인터넷 상점과 연계하여 서비스를 제공하는 경우의 전자 화폐 발행 및 서비스 이용을 위해 해쉬 함수만으로 저렴하면서도 안전하게 전자 화폐를 전송하여, 광고주나 설문에 의한 여론 조사를 하는 경우 광고를 읽는 사람이나 설문에 대답하는 사람에게 전자 상거래 응용 분야에서 사용할 수 있는 전자 화폐를 발행하거나 일정 금액이 되는 경우 실세계의 현금으로 환전하여 줌으로써, 광고를 보는 것을 촉진시키고, 설문지 응답자 수를 증가시키며, 발행된 전자 화폐를 전자 상거래 서비스 이용으로 유도할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1

인터넷 상에서 소액 지불을 가능하게 하는 소액 전자 지불 기반 온라인 서비스 방법에 있어서,

인터넷 상거래 서비스를 이용하고자 하는 사용자의 등록 처리를 하는 제 1 과정과;

상기 제 1 과정의 사용자에게 지불 센터에서 전자 화폐를 발행하는 제 2 과정과;

상기 제 2 과정에서 발행된 전자 화폐로 사용자가 서비스 이용료를 지불하는 제 3 과정을 포함하는 것을 특징으로 하는 소액 전자 지불 기반 온라인 서비스 방법.

9-7

청구항 2

제 1 항에 있어서,

상기 제 1 과정은, 구매자가 사용자 정보를 지불 센터로 전송하여 사용자 등록을 요구하는 제 1 단계와;

상기 제 1 단계의 사용자 등록 요구에 의해 지불 센터가 사용자 등록을 수행한 후 구매자에게 사용자 등록을 통지하는 제 2 단계를 포함하는 것을 특징으로 하는 소액 전자 지불 기반 온라인 서비스 방법.

청구항 3

제 1 항에 있어서,

상기 제 2 과정은, 인터넷 상점 등에서 제공하는 설문지 응답, 퀴즈 풀기 또는 광고를 읽은 후 구매자가 판매자에게 전자 화폐 발행을 요청하는 제 1 단계와;

상기 제 1 단계의 전자 화폐 발행 요청 메시지를 수신한 판매자가 상기 구매자의 응답을 조사한 후 전자 화폐 발행의 근거가 되는 트랜잭션 ID와 발행 금액 등을 구매자에게 전송하여 전자 화폐 발행 요청에 응답하는 제 2 단계와;

구매자가 지불 센터로 트랜잭션 ID를 전송하여 지불 센터를 초기화하는 제 3 단계와;

상기 구매자가 보유하고 있는 전자 화폐 ScripType와 지불 센터가 공유하는 비밀 정보 Custom_secret의 연접에 대한 해쉬 값을 전송하여 전자 화폐의 무결성 및 메시지 인증 기능을 수행하여 전자 화폐를 발행 개시하는 제 4 단계와;

상기 제 4 단계의 메시지를 수신한 상기 지불 센터가 전자 화폐의 유효성을 해쉬 값 검사에 의해 수행하며 정상적인 경우 화폐를 갱신하여 갱신된 화폐 newScripType와 비밀 정보 Custom_secret의 연접에 대한 해쉬 값을 상기 구매자로 전송하여 전자 화폐의 무결성 및 메시지 인증 기능을 수행하여 전자 화폐를 발행하는 제 5 단계와;

상기 제 5 단계에서 지불 센터가 발행한 전자 화폐의 무결성등을 수행후 구매자가 보유하는 전자 화폐를 지불 센터에 전송하고, 상기 지불 센터로 하여금 상기 구매자가 보유하는 전자 화폐에 대한 인증을 제공하여 전자 화폐 확인 및 결과를 통지하는 제 6 단계와;

상기 제 6 단계가 완료된 후, 전자 화폐 지불 종료 메시지를 구매자에게 전송하여 지불 센터를 종료하는 제 7 단계를 포함하는 것을 특징으로 하는 소액 전자 지불 기반 온라인 서비스 방법.

청구항 4

제 1 항에 있어서,

상기 제 3 과정은, 구매자가 판매자에게 인터넷 상점이 제공하는 서비스를 요청하는 제 1 단계와;

판매자가 서비스 이용에 대한 서비스 이용료 지불을 요구하는 메시지를 상기 구매자에게 전송하여 서비스 지불 정보를 통지하는 제 2 단계와;

상기 제 2 단계의 서비스 지불 메시지를 수신한 구매자가 트랜잭션을 식별하므로써 지불 센터를 초기화하는 메시지를 지불 센터로 전송하여 지불 센터를 초기화하는 제 3 단계와;

상기 제 3 단계의 메시지로부터 수신한 서비스 이용료 정보에 근거하여 구매자가 주문 정보와 전자 화폐를 지불 센터로 전송하여 서비스 이용료를 지불하는 제 4 단계와;

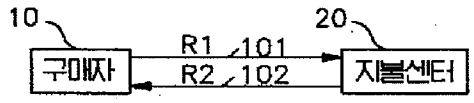
상기 제 4 단계의 주문 정보과 전자 화폐 메시지를 수신한 지불 센터가 전자 화폐를 재발행한 후, 재발행한 전자 화폐를 비밀 정보와의 해쉬값으로 구매자에게 전송하여 서비스 이용료 지불을 처리하는 제 5 단계와;

상기 제 5 단계에서 비밀 정보와의 해쉬값으로 전송된 전자 화폐를, 상기 제 5 단계 이전에 구매자가 보유하고 있던 화폐와 상기 제 2 단계에서 제공된 서비스 이용료에 근거하여 갱신된 화폐를 확인하고, 새로이 갱신된 전자 화폐의 수락 여부를 지불 센터에 전송하여 지불 처리 확인 결과를 통지하는 제 6 단계와;

상기 구매자가 선택한 서비스를 전송하는 제 7 단계를 포함하는 것을 특징으로 하는 소액 전자 지불 기반 온라인 서비스 방법.

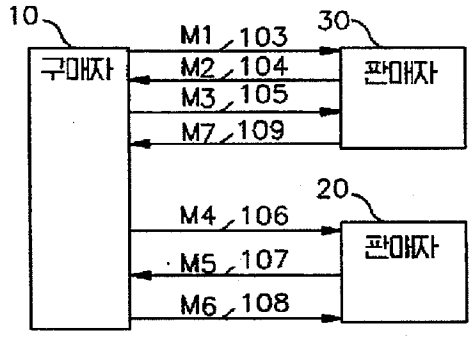
도면

도면1

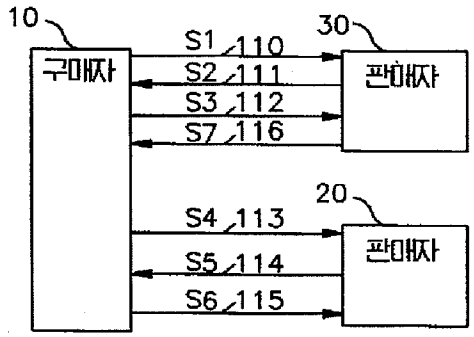


9-8

도면2


10
구매자
M1 103
M2 104
M3 105
M7 109
30
판매자
M4 106
M5 107
M6 108
20
판매자

도면3


10
구매자
S1 110
S2 111
S3 112
S7 116
30
판매자
S4 113
S5 114
S6 115
20
판매자

9-9